REMARKS

Response to Claim Rejections Under 35 U.S.C. §102(b)

The Office has rejected claims 1-4, 12, 14, 16-19, 25, and 27-29 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,774,650 to Chapman et al. If examination at the initial stage does not produce a *prima facie* case of unpatentability, then without more, the applicant is entitled to the grant of the patent. See *In re Oetiker*, 977 F. 2d 1443 (Fed. Cir. 1992). Under 35 U.S.C. § 102, anticipation requires that there is no difference between the claimed invention and reference disclosure, as viewed by a person of ordinary skill in the field of the invention. See *Scripps Clinic & Research Foundation v. Genentech, Inc.*, 927 F.2d 1565. Anticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim. In deciding the issue of anticipation, the trier of fact must identify the elements of the claims, determine their meaning in light of the specification and prosecution history, and identify corresponding elements disclosed in the allegedly anticipating reference. *See Lindemann Maschinenfabrik GmbH v. American Hoist & Derrick Co.*, 730 F.2d 1452.

Regarding Applicants' claims, Applicants' claims recite a method and system for verifying the identities of new users of a computer system using similarity searching in order to detect user identity fraud, as contrasted to the Chapman reference which discloses a method for controlling access to a networked computer system by username and password. These differences account for the Applicants' claim limitations that are not found in the Chapman reference. The tables shown below show a side-by-side comparison of the limitations of Applicants' claims with the citations relied on by the Office for rejecting Applicants' claims.

It should be noted that the meaning of the term "similarity searching" is based on the use of a similarity search engine disclosed in paragraph 0009 of Applicants' specification as U.S.

Patent Application No. 09/401,101, filed on September 22, 1999, which is incorporated by reference into Applicants' specification. U.S. Patent Application No. 09/401,101 issued as U.S. Patent No. 6,618,727 on September 9, 2003. The information incorporated is as much a part of the application as filed as if the text were repeated in the application, and should be treated as part of text of the application as filed. See MPEP 2163.07(b).

Similarity searching according to U.S. Patent No. 6,618,727 is a computer-implemented method for detecting and scoring similarities between documents in a source database and a search criterion such as new user profile data. It uses a hierarchy of parent and child categories to be searched, linking each child category with its parent category, which may be likened to a tree type structure with parent and child objects. Source database documents are converted into hierarchical database documents having parent and child objects with data values organized using the hierarchy of parent and child categories to be searched. For each child object, a child object score is calculated that is a quantitative measurement of the similarity between child objects in the hierarchical database documents and the search criteria. A parent object score are computed from its child object scores. A user may select from a list of unique algorithms for determining child object scores and parent object scores. Calculating a score comprises determining a number for the score that represents how similar and dissimilar the source value is to the search criteria such as the new user profile data. The calculated score is a quantitative measure of the similarity between the source data and search criteria, and may, for example, take on any value between the numbers zero and one.

The first element of Applicants' claim 1 recites the limitation, "receiving at least one identity attribute from the new-user". See row 1 of Table 1 for a side-by-side comparison of this first limitation of claim 1 with the passage from the Chapman reference that the Office asserts is equivalent. Applicants contend that this claim limitation is not explicit, implicit or inherent in the

passage in Chapman cited by the Office, as shown in Table 1. The at least one identity attribute in this limitation is not constrained to be user names and passwords for gaining access to a computer system, as cited by the Office in column 1, lines 17-20 of the Chapman reference. Note that during patent examination, the pending claims must be given their broadest reasonable interpretation consistent with the specification. *In re Hyatt*, 211 F.3d 1367, 1372 (Fed. Cir. 2000). While the Chapman reference relies on usernames and passwords assigned by a system owner for authorizing access, Applicants claimed invention relies on at least one identity attribute to verify a new user identity, where the dictionary definition of attribute is any inherent characteristic or object closely associated with or belonging to a specific person. Applicants' at least one identity attribute is input by a new user prior to allowing or denying the new user access to the computer system, for determining that the new user is the person identified by the identity attribute. Since, at the time a new user enters the at least one identity attribute, the new user has not given access to the computer system, the new user has not been assigned a username and password for system access by a system owner. Applicants' at least one identity attribute is used to determine if the new user has been involved in fraudulent activities in the past, prior to allowing system access via a username and password information, as described in the Chapman reference for gaining access to a computer system. There is no disclosure in Applicants' claimed invention of supplying a username and password when the user logs on, as disclosed in the Chapman reference. All users of a computer system must enter the access information listed in the Chapman reference every time a user wishes to gain access to the computer system. The at least one identity attribute profile data of Applicants' disclosure is only required by a new user, prior to allowing initial system access by a new user, to determine if the new user qualifies for access to the computer system. Once a new user qualifies for access to the computer system resulting from a negative similarity match according to Applicants' invention, the new user no

longer needs to be re-qualified by inputting identity attribute profile data. Once a new user has been qualified by a negative similarity match and allowed to gain access to the computer system, the new user is no longer a new user, and becomes a normally authorized user as disclosed in the Chapman reference. Therefore, when the meaning of this limitation of Applicants' claim 1, namely, "receiving at least one identity attribute from the new-user" is given it broadest reasonable interpretation, this limitation is not found in the Chapman reference cited by the Office, because the new user has not been assigned a user name and password by a system owner. As shown in row 1 of Table 1, there is no correspondence between the first limitation of Applicants' claim 1, and the passages in the Chapman reference cited by the Office.

The second and third elements of Applicants' claim 1 recite the limitation, "similarity searching the at least one new user identity attribute against at least one database of denied user identity attributes" and "receiving a similarity search result", respectively. As described above, U.S. Patent No. 6,618,727, which is incorporated herein by reference, discloses a similarity search engine that may be used for similarity searching by comparing two documents to determine an indicia of similarity that provides a quantitative measure of how alike the two documents are, such as new user identity attributes and denied user identity attributes. This similarity search engine is used to similarity search the identity attributes against denied user identity attributes and provide a similarity search result that includes indicia of similarity. The denied user identity attributes contain identity attributes of users that have been removed or suspended from the system in the past. If a new user identity attribute has a positive similarity match to a suspended-user's identity attributes, the new user is denied access to the computer system. There is no disclosure in the Chapman reference of these limitations. As shown in rows 2-6 of Table 1, there is no correspondence between the second and third limitations of Applicants' claim 1, and the passages in the Chapman reference cited by the Office.

The fourth and fifth element of Applicants' claim 1 recite the limitations "determining a positive or negative similarity match between at least one new user identity attribute and the denied user identity attributes based on the similarity search result" and "allowing a new user to access the computer system, where a negative similarity match has been determined", respectively. There is no disclosure in the Chapman reference of determining a positive or negative similarity match between identity attribute profile data and suspended-users identity attribute profile data based on the similarity search result. There is also no disclosure in the Chapman reference of allowing a new user access to the system where a negative similarity match has been determined. The Chapman reference discloses validating a user account by (positively) matching a supplied user name with a username in a valid account, and authenticating the user by comparing the true password corresponding to the validated username with a password supplied by the user who is attempting to gain access. As shown in rows 2-6 of Table 1, there is no correspondence between the fourth and fifth limitations of Applicants' claim 1, and the passages in the Chapman reference cited by the Office.

The sixth element of Applicants' claim 1 recites the limitation "denying the new user access to the computer system where a positive similarity match has been determined." There is no disclosure in the Chapman reference of a denying a new user access to the computer system based on a positive similarity match. In fact, the Chapman reference allows access to the system when a positive match exists between a supplied username and an existing account username. The Office cites column 6, line 58-63 of the Chapman reference as disclosing Applicants' second through sixth limitations of claim 1. See rows 2-6 of Table 1 for a side-by-side comparison of the second through sixth limitation of claim 1 with the passage from the Chapman reference that the Office asserts is equivalent. Applicants contend that this claim limitation is not explicit, implicit or inherent in the passage in Chapman cited by the Office, as shown in Table 1. This passage

describes conventional methods for validating a user account by exact matching of usernames or user numbers provided by a user during a login sequence with data stored in a database file containing unauthorized or temporarily authorized user names or user numbers. Access to the computer system by a user is authenticated by exact comparison of the encrypted true password with that supplied by a user attempting to logon, and establishing exact user credentials stored in a database. This cited passage requires positive exact matching of usernames and passwords for allowing access, which may be performed by conventional database management systems. Where a positive exact match is found, a user is allowed access to the computer system. Whereas, with Applicants' claimed invention, when a positive similarity match between the at least one new user identity attribute and a denied user identity attributes is determined, access by the new user is denied. There is no disclosure of similarity searching as disclosed by Applicants in this cited passage, and furthermore, a similarity search would not be applicable or desirable to this application, since persons other than an authenticated user may gain access to the computer system by providing similar usernames and passwords. There is also no disclosure in the Chapman reference of similarity searching identity attribute profile data against denied-users identity attribute profile data. There is no disclosure of either similarity searching or of denied-users identity profile data in the Chapman reference, which merely describes authorized users, temporarily unauthorized users, temporarily authorized users and a privileged user for controlling the authorization and unauthorization process. There is no disclosure in the cited passage in the Chapman reference of receiving a similarity search result. Furthermore, in order to accomplish this limitation, a similarity search engine like that disclosed in U.S. Patent No. 6,618,727 would be required. As shown in rows 2-7 of Table 1, there is no correspondence between the sixth limitation of Applicants' claim 6, and the passages in the Chapman reference cited by the Office.

It should be especially noted that for conventional applications involving authenticating usernames and passwords for computer access, exact matching of these parameters is a requirement every time a user desires access to the system. In contrast, when attempting to uncover computer access through fraudulent means, non-exact or similarity matching is desirable in order to make a determination of fraudulent activity based on degrees of similarity on a one-time basis for new users.

Since every element of Applicants' claimed invention, arranged as in the independent claim 1 are not found implicitly, explicitly or inherently in the single reference of Chapman, the Office has failed to substantiate a *prima facie* case for anticipation and Chapman et al does not anticipate Applicants' independent claim 1. Therefore the rejection of claim 1 should be withdrawn. Furthermore, claims 2-14 and 28 are either directly or indirectly dependent upon independent claim 1. These dependent claims incorporate all the limitations of the independent claim upon which they depend while providing further unique and non-obvious recitations. Since the rejection of claim 1 is not supported by the Chapman disclosure, the rejections of these dependent claims 2-14 and 28 as anticipated are also not supported by the Chapman reference and should be withdrawn. Applicants request withdrawal of the rejection of claims 1-14 and 28, reconsideration and allowance of the application.

COMPARISON OF CLAIM 1 LIMITATIONS WITH PASSAGES CITED BY THE OFFICE		
CLAIM LIMITATIONS	CITATION	OFFICE ASSERTED EQUIVALENT IN CHAPMAN
1. "a. receiving at least one identity attribute from the new user"	Chapman: Column 1, Lines 17-20	"In most multiuser systems, a file or files listing valid usernames, or valid combinations of usernames and passwords are kept, and a user gains access to the system by supplying such a name and password when he logs on."
2. "b. similarity searching the at least one new-user identity attribute against at least one database of denied-user identity attributes" 3. "c. receiving a similarity search result" 4. "d. determining a positive or negative similarity match between the at least one new-user identity attribute and the denied-user identity attributes based on the similarity search results" 5. "e. allowing the new-user to access the computer system, where a negative similarity match has been determined" 6. "f. denying the new-user access to the computer system, where a positive similarity match has been determined"	Chapman: Column 6, Lines 58-63	"For example, a list of temporarily unauthorized, or temporarily authorized usernames could be constructed (the latter could even include invalid usernames, since the account validating step 44 of the logon sequence would ensure these were not admitted), or the user number 33 could be required to be within a specified interval."

TABLE 1

Regarding Applicants' dependent claims 2-14 and 28, claims 2-14 and 28 are either directly or indirectly dependent upon independent claim 1. These dependent claims incorporate all the limitations of the independent claim upon which they depend while providing further unique and non-obvious recitations. Since it has been shown above that the rejection of claim 1 is not supported by the Chapman disclosure and claim 1 is not anticipated, the rejections of these dependent claims 2-14 and 28 as anticipated are also not supported by the Chapman reference and should be withdrawn. The discussion below concerns dependent claims 2-4, 12, 14 and 28 which stand rejected as anticipated under 35 U.S.C. § 102(b). See Table 2 for a side-by-side comparison of the limitations of Applicants' claims 2-4, 12 and 14 with the citations relied on by the Office for rejecting these claims.

Considering further Applicants' dependent claim 2, claim 2 recites the limitation, "wherein the at least one new-user identity attribute comprises a new-user profile." The Office has cited column 5, line 65 through column 6, line 3 as disclosing the limitation of claim 2. See row 1 of Table 2A for a side-by-side comparison of the limitation of claim 2 with the passage cited by the Office. Claim 2 describes the at least one new user identity attribute, described above and defined in a dictionary as any inherent characteristic or object closely associated with or belonging to a specific person, as comprising a new user profile. The profile cited by the Office describes a computer file /etc/profile used by a shell program to personalize a user's work environment in a UNIX operating system. Although the names are the same, the use of "profile" in the context of Applicants' claims and the use of "profile" in the context of the Chapman disclosure are entirely different. Contrast Applicants' use of a profile comprising at least one new user identity attribute to qualitatively identify a new user with Chapman's use of a profile to describe a UNIX operating system file for configuring a user's work environment. There is no

disclosure in the Chapman reference of the limitation of Applicants' claim 2. As shown in row 1 of Table 2A, there is no correspondence between the limitations of Applicants' claim 2, and the passages in the Chapman reference cited by the Office.

Considering further Applicants' claim 3 and claim 4, claim 3 recites the limitation, "wherein the at least one database of denied-user identity attributes comprises at least one database of denied-user profiles." and claim 4 recites the limitation, "wherein the step of similarity searching comprises similarity searching the new-user profile against the at least one denied-user profile database." The Office has cited column 6, line 58 through column 7, line 6 as disclosing the limitation of claims 3 and 4. See rows 2 and 3 of Table 2A for a side-by-side comparison of the limitation of claims 3 and 4 with the passage cited by the Office. Claim 3 describes at least one database of denied user identity attributes that comprises at least one database of denied user profiles. As described above in relation to claim 2, the UNIX operating system profile files for configuring a user's work environment bear no relationship to Applicants' denied user profiles comprising denied user identity attributes that identify any inherent characteristic or object closely associated with or belonging to a specific person. Claim 4 describes similarity searching a new user profile against at least one denied user profile database. There is no disclosure in Chapman of similarity searching a new user profile against a denied user database. There is no suggesting or teaching of similarity searching in the Chapman reference, nor is there any disclosure of a denied user profile database comprising denied user identity attributes. A database of temporarily unauthorized usernames is not a denied user profile database. There is no disclosure in the Chapman reference of the limitations of Applicants' claims 3 and 4. As shown in rows 2 and 3 of Table 2A, there is no correspondence between the limitations of Applicants' claims 3 and 4, and the passages in the Chapman reference cited by the

Office.

Considering further Applicants' claim 12, claim 12 recites the limitation, "after determining whether a positive or negative similarity match exists, the steps of: adding the new-user identity to at least one database of valid user identities, where a negative similarity match has been determined; and adding the new-user identity attributes to the at least one database of denied-user identity attributes, where a positive similarity match has been determined." The Office cited column 4, lines 13-22, column 6, lines 23-25, and column 6, lines 56-64 as disclosing the limitations of claim 12. See row 4 in Table 2B for a side-by-side comparison of the limitation of claim 12 with the passage cited by the Office. The passage cited by the Office in column 4, lines 13-22 of Chapman describe creating a user account for enabling system access and a user's home directory for storing user programs and data. There is no relationship between this Chapman citation for creating a new user account and Applicants' adding a new user identity to at least one database of valid user identities, where a negative similarity match has been determined. The passage cited by the Office in column 6, lines 23-25 of Chapman describe temporarily restricting access to a system by determining if the user of the access control program is privileged. There is no relationship between a check to determine if the user of the access control program is privileged, as recited in Chapman, and adding a new user identity to at least one database of valid user identities where a negative similarity match has been determined, as recited in Applicants' claim 12. The passage cite by the Office in column 6, lines 56-64 of Chapman describe creating a definition of temporarily unauthorized users. There is no relationship between creating a definition of temporarily unauthorized users, as recited in Chapman, and adding new user identity attributes to the at least one database of denied user identity attributes where a positive similarity match has been determined, as recited in

Applicants' claim 12. There is no disclosure in the Chapman reference of any of the limitations of Applicants' claim 12. As shown in row 4 of Table 2B, there is no correspondence between the limitations of Applicants' claim 12, and the passages in the Chapman reference cited by the Office.

Considering Applicants' claim 14, claim 14 recites the limitation, "wherein the similarity search result comprises at least one hierarchical document stored in the at least one database of denied-user identity attributes." The Office cited column 6, line 65 through column 7, line 3 as disclosing the limitations of claim 12. See row 5 in Table 2B for a side-by-side comparison of the limitation of claim 12 with the passage cited by the Office. The passage cited by the Office in Chapman describes modifying the system-wide profile by addition of code to the system-wide profile file /etc/profile used by a shell program for defining a user's environment to log off a user if the user is temporarily unauthorized. There is no disclosure in Chapman of a similarity search result or of a hierarchical document stored in a database of denied-user identity attributed. As described above in relation to claim 2, the UNIX operating system profile files for configuring a user's work environment bear no relationship to Applicants' denied user profiles comprising denied user identity attributes that identify any inherent characteristic or object closely associated with or belonging to a specific person, as recited in claim 14. There is no disclosure in the Chapman reference of any of the limitations of Applicants' claim 14. As shown in row 14 of Table 2B, there is no correspondence between the limitations of Applicants' claim 14, and the passages in the Chapman reference cited by the Office.

Considering Applicants' claim 28, claim 28 recites the limitation, "A computer-readable medium containing instructions for controlling a computer system to implement the method of claim 1." As described above, claim 1 is not anticipated by the Chapman reference. Since claim

28 is dependent on claim 1 and incorporates all the limitations of claim 1, claim 28 is also not anticipated by the Chapman reference.

As described above, the limitations of Applicants claims 2-4, 12, 14 and 28 are not disclosed in the Chapman reference. Therefore, claims 2-4, 12, 14 and 28 are not anticipated under 35 U.S.C. 102(b) by the Chapman reference.

COMPARISON OF DEPENDENT CLAIMS 2-4, 12 AND 14 LIMITATIONS WITH PASSAGES CITED BY THE OFFICE		
CLAIM LIMITATIONS	CITATION	OFFICE ASSERTED EQUIVALENT IN CHAPMAN
1. Claim 2 "wherein the at least one new-user identity attribute comprises a new-user profile."	Chapman: Column 5, Line 65 through Column 6, Line 3	The cited passage is part of a description of the UNIX logon sequence, as the title in column 5, line 12 illustrates, and is based on a conventional AIX operating system logon sequence. As described in column 4, lines 49-55, "In UNIX, a shell is a command interpreter that must be running for a user to have an interactive logon session." The citation in the Chapman reference describes "programs referred to as profiles are run 70." These programs are described as system-wide profile /etc/profile 72, and a file called profile in the user's home directory that is run subsequently by a shell program. As is well-known to UNIX operating system programmers, the profile file /etc/profile are system-wide profile files that contain initialization data used by the login shell at login time for personalizing a user's work environment by setting exported environment variables, definitions settings and terminal mode. A profile file includes at least a PATH statement and a MANPATH statement.
2. Claim 3 "wherein the at least one database of denied-user identity attributes comprises at least one database of denied-user profiles."	Chapman: Column 6, Line 58 through Column 7, Line 6	The cited passage includes a description of creating a definition of temporarily unauthorized or temporarily authorized usernames. The passage also describes the addition of code to the system-wide profile file /etc/profile used by the shell program for defining a user's environment (as described above) to log off a user if the user is temporarily unauthorized.
3. Claim 4 "wherein the step of similarity searching comprises similarity searching the new-user profile against the at least one denied-user profile database."		

TABLE 2A

COMPARISON OF DEPENDENT CLAIMS 2-4, 12 AND 14 LIMITATIONS WITH PASSAGES CITED BY THE OFFICE		
CLAIM LIMITATIONS	CITATION	OFFICE ASSERTED EQUIVALENT IN CHAPMAN
4. Claim 12 "further comprising, after determining whether a positive or negative similarity match exists, the steps of: adding the new-user identity to at least one database of valid user identities, where a negative similarity match has been determined; and adding the new-user identity attributes to the at least one database of denied-user identity attributes, where a positive similarity match has been determined."	Chapman: Column 4, Lines 13-22	The cited passage describes adding a new user to a UNIX system by creating a "user account" consisting of two parts: an entry for enabling system access in a file entitled /etc/password that defines accounts and their characteristics; and a user's home directory for storing user programs and data.
	Chapman: Column 6, Lines 23-25	The cited passage describes a method for temporarily restricting access to a system that comprises a check to determine if the user of the access control program is privileged. In UNIX terms, the privileged user must have superuser authority, such as the system owner.
	Chapman: Column 6, Lines 56-64	"Check (users to be permitted access) and create 89 a definition of temporarily unauthorized users, by any appropriate method. For example, a list of temporarily unauthorized, or temporarily authorized usernames could be constructed (the latter could even include invalid usernames, since the account validating step 44 of the logon sequence would ensure these were not admitted), or the user number 33 could be required to be within a specified interval. The privileged user executing this program would always included."
5. Claim 14 "wherein the similarity search result comprises at least one hierarchical document stored in the at least one database of denied-user identity attributes."	Chapman: Column 6, Line 65 through Column 7, Line 3	The cited passage describes the step of modifying the system-wide profile by the addition of code to the system-wide profile file /etc/profile used by the shell program for defining a user's environment (as described above) to log off a user if the user is temporarily unauthorized.

TABLE 2B

Considering Applicants independent claim 16, the first element of Applicants' claim 16 recites the limitation, "receiving at least one identity attribute from the new-user". See row 1 of Table 3A for a side-by-side comparison of this first limitation of claim 16 with the passage from the Chapman reference that the Office asserts is equivalent. Applicants contend that this claim limitation is not explicit, implicit or inherent in the passage in Chapman cited by the Office, as shown in Table 3A. The at least one identity attribute in this limitation is not constrained to be user names and passwords for gaining access to a computer system, as cited by the Office in column 1, lines 17-20 of the Chapman reference. Note that during patent examination, the pending claims must be given their broadest reasonable interpretation consistent with the specification. *In re Hyatt*, 211 F.3d 1367, 1372 (Fed. Cir. 2000). While the Chapman reference relies on usernames and passwords assigned by a system owner for authorizing access, Applicants claimed invention relies on at least one identity attribute to verify a new user identity, where the dictionary definition of attribute is any inherent characteristic or object closely associated with or belonging to a specific person. Applicants' at least one identity attribute is input by a new user prior to allowing or denying the new user access to the computer system, for determining that the new user is the person identified by the identity attribute. Since, at the time a new user enters the at least one identity attribute, the new user has not given access to the computer system, the new user has not been assigned a username and password for system access by a system owner. Applicants' at least one identity attribute is used to determine if the new user has been involved in fraudulent activities in the past, prior to allowing system access via a username and password information, as described in the Chapman reference for gaining access to a computer system. There is no disclosure in Applicants' claimed invention of supplying a username and password when the user logs on, as disclosed in the Chapman reference. All users of a computer system must enter the access information listed in the

Chapman reference every time a user wishes to gain access to the computer system. The at least one identity attribute profile data of Applicants' disclosure is only required by a new user, prior to allowing initial system access by a new user, to determine if the new user qualifies for access to the computer system. Once a new user qualifies for access to the computer system resulting from a negative similarity match according to Applicants' invention, the new user no longer needs to be re-qualified by inputting identity attribute profile data. Once a new user has been qualified by a negative similarity match and allowed to gain access to the computer system, the new user is no longer a new user, and becomes a normally authorized user as disclosed in the Chapman reference. Therefore, when the meaning of this first limitation of Applicants' claim 16, namely, "receiving at least one identity attribute from the new-user" is given it broadest reasonable interpretation, this limitation is not found in the Chapman reference cited by the Office, because the new user has not been assigned a user name and password by a system owner. As shown in row 1 of Table 3A, there is no correspondence between the first limitation of Applicants' claim 16, and the passages in the Chapman reference cited by the Office.

The second and third elements of Applicants' claim 16 recite the limitation, "similarity searching the at least one new user identity attribute against at least one database of denied user identity attributes" and "receiving a similarity search result", respectively. As described above, U.S. Patent No. 6,618,727, which is incorporated herein by reference, discloses a similarity search engine that may be used for similarity searching by comparing two documents to determine an indicia of similarity that provides a quantitative measure of how alike the two documents are, such as new user identity attributes and denied user identity attributes. This similarity search engine is used to similarity search the identity attributes against denied user identity attributes and provide a similarity search result that includes indicia of similarity. The denied user identity attributes contain identity attributes of users that have been removed or

suspended from the system in the past. If a new user identity attribute has a positive similarity match to a suspended-user's identity attributes, the new user is denied access to the computer system. There is no disclosure in the Chapman reference of these limitations.

The fourth and fifth element of Applicants' claim 16 recite the limitations "determining a positive or negative similarity match between at least one new user identity attribute and the denied user identity attributes based on the similarity search result" and "allowing a new user to access the computer system and adding the new user identity to at least one database of valid user identities, where a negative similarity match has been determined", respectively. There is no disclosure in the Chapman reference of determining a positive or negative similarity match between identity attribute profile data and suspended-users identity attribute profile data based on the similarity search result. There is also no disclosure in the Chapman reference of allowing a new user access to the system where a negative similarity match has been determined. The Chapman reference discloses validating a user account by (positively) matching a supplied user name with a username in a valid account, and authenticating the user by comparing the true password corresponding to the validated username with a password supplied by the user who is attempting to gain access.

The Office cites column 6, line 58-63 of the Chapman reference as disclosing Applicants' second through fifth limitations of claim 16. See rows 2-5 of Table 3A for a side-by-side comparison of the second through fifth limitation of claim 16 with the passages from the Chapman reference that the Office asserts is equivalent. Applicants contend that this claim limitation is not explicit, implicit or inherent in the passage in Chapman cited by the Office, as shown in Table 3A. This passage describes conventional methods for validating a user account by exact matching of usernames or user numbers provided by a user during a login sequence with data stored in a database file containing unauthorized or temporarily authorized user names

or user numbers. Access to the computer system by a user is authenticated by exact comparison of the encrypted true password with that supplied by a user attempting to logon, and establishing exact user credentials stored in a database. This cited passage requires positive exact matching of usernames and passwords for allowing access, which may be performed by conventional database management systems. Where a positive exact match is found, a user is allowed access to the computer system. Whereas, with Applicants' claimed invention, when a positive similarity match between the at least one new user identity attribute and a denied user identity attributes is determined, access by the new user is denied. There is no disclosure of similarity searching as disclosed by Applicants in this cited passage, and furthermore, a similarity search would not be applicable or desirable to this application, since persons other than an authenticated user may gain access to the computer system by providing similar usernames and passwords. There is also no disclosure in the Chapman reference of similarity searching identity attribute profile data against denied-users identity attribute profile data. There is no disclosure of either similarity searching or of denied-users identity profile data in the Chapman reference, which merely describes authorized users, temporarily unauthorized users, temporarily authorized users and a privileged user for controlling the authorization and unauthorization process. There is no disclosure in the cited passage in the Chapman reference of receiving a similarity search result. Furthermore, in order to accomplish this limitation, a similarity search engine like that disclosed in U.S. Patent No. 6,618,727 would be required. As shown in rows 2-5 of Table 3A, there is no correspondence between the second through fifth limitations of Applicants' claim 16, and the passages in the Chapman reference cited by the Office.

The Office also cited column 4, lines 13-22 and column 6, lines 23-25 as disclosing the second through fifth limitations of claim 16. See rows 2-5 in Table 3A for a side-by-side comparison of the limitation of claim 16 with the passage cited by the Office. The passage cited

by the Office in column 4, lines 13-22 of Chapman describe creating a user account for enabling system access and a user's home directory for storing user programs and data. There is no relationship between this Chapman citation for creating a new user account and Applicants' adding a new user identity to at least one database of valid user identities, where a negative similarity match has been determined. The passage cited by the Office in column 6, lines 23-25 of Chapman describe temporarily restricting access to a system by determining if the user of the access control program is privileged. There is no relationship between a check to determine if the user of the access control program is privileged, as recited in Chapman, and adding a new user identity to at least one database of valid user identities where a negative similarity match has been determined, as recited in Applicants' claim 16. As shown in rows 2-5 of Table 3A, there is no correspondence between the second through fifth limitations of Applicants' claim 16, and the passages in the Chapman reference cited by the Office.

Considering the sixth and seventh limitations of Applicants' claim 16, shown in row 6 and 7 of Table 3B, the Office has not cited any passage in Chapman of providing a secondary review where a positive similarity match has been determined. The Office has also not cited any passage in Chapman of allowing a new user access to the system and adding the new user identity to a valid user identity database, where the positive similarity match is not verified. Neither of these limitations of claim 16 are found in the Chapman reference.

The Office also cited column 6, lines 56-64 as disclosing the eighth limitations of claim 16. See row 8 in Table 3B for a side-by-side comparison of this limitation of claim 16 with the passage cited by the Office. The passage cite by the Office in column 6, lines 56-64 of Chapman describe creating a definition of temporarily unauthorized users. There is no relationship between creating a definition of temporarily unauthorized users, as recited in Chapman, and the limitation of denying the new user access to the computer system and adding new user identity attributes to

the at least one database of denied user identity attributes where a positive similarity match has been determined, as recited in Applicants' eighth limitation of claim 16. There is no disclosure in the Chapman reference of any of the limitations of Applicants' claim 16. As shown in row 8 of Table 3B, there is no correspondence between the eighth limitation of Applicants' claim 16, and the passages in the Chapman reference cited by the Office.

It should be especially noted that for conventional applications involving authenticating usernames and passwords for computer access, exact matching of these parameters is a requirement every time a user desires access to the system. In contrast, when attempting to uncover computer access through fraudulent means, non-exact or similarity matching is desirable in order to make a determination of fraudulent activity based on degrees of similarity on a one time basis for new users.

Since every element of Applicants' claimed invention, arranged as in independent claim 16, are not found implicitly, explicitly or inherently in the single reference of Chapman, the Office has failed to substantiate a *prima facie* case for anticipation and Chapman et al does not anticipate Applicants' independent claim 16. Therefore the rejection of claim 16 should be withdrawn. Furthermore, claims 17-25 and 29 are either directly or indirectly dependent upon independent claim 16. These dependent claims incorporate all the limitations of the independent claim upon which they depend while providing further unique and non-obvious recitations. Since the rejection of claim 16 is not supported by the Chapman disclosure, the rejections of these dependent claims 17-25 and 29 as anticipated are also not supported by the Chapman reference and should be withdrawn. Applicants request withdrawal of the rejection of claims 16-25 and 29, reconsideration and reexamination of the application.

COMPARISON OF CLAIM 16 LIMITATIONS WITH PASSAGES CITED BY THE OFFICE		
CLAIM LIMITATIONS	CITATION	OFFICE ASSERTED EQUIVALENT IN CHAPMAN
1. "a. receiving at least one identity attribute from the new user"	Chapman: Column 1, Lines 17-20	"In most multiuser systems, a file or files listing valid usernames, or valid combinations of usernames and passwords are kept, and a user gains access to the system by supplying such a name and password when he logs on."
2. "b. similarity searching the at least one new-user identity attribute against at least one database of denied-user identity attributes" 3. "c. receiving a similarity search result" 4. "d. determining a positive or negative similarity match between the at least one new-user identity attribute and the denied-user identity attributes based on the similarity search results" 5. "e. allowing the new-user to access the computer system and adding the new-user identity to at least one database of valid user identities, where a negative similarity match has been determined"	Chapman: Column 6, Lines 58-63	"For example, a list of temporarily unauthorized, or temporarily authorized usernames could be constructed (the latter could even include invalid usernames, since the account validating step 44 of the logon sequence would ensure these were not admitted), or the user number 33 could be required to be within a specified interval."
	Chapman: Column 4, Line 13-22	The cited passage describes adding a new user to a UNIX system by creating a "user account" consisting of two parts: an entry for enabling system access in a file entitled /etc/password that defines accounts and their characteristics; and a user's home directory for storing user programs and data.
	Chapman: Column 6, Line 23-25	The cited passage describes a method for temporarily restricting access to a system that comprises a check to determine if the user of the access control program is privileged. In UNIX terms, the privileged user must have superuser authority, such as the system owner.

TABLE 3A

COMPARISON OF CLAIM 16 LIMITATIONS WITH PASSAGES CITED BY THE OFFICE		
CLAIM LIMITATIONS	CITATION	OFFICE ASSERTED EQUIVALENT IN CHAPMAN
6. "f. where a positive similarity match has been determined, verifying the positive similarity match via a secondary review" 7. "g. allowing the new-user to access the computer system and adding the new-user identity to at least one database of valid user identities, where the positive similarity match is not verified"	NONE	NONE
8. "h. denying the new-user access to the computer system and adding the at least one new-user identity attribute to at least one database of denied-user identity attributes, where the positive similarity match is verified"	Chapman: Column 6, Lines 56-64	"Check (users to be permitted access) and create 89 a definition of temporarily unauthorized users, by any appropriate method. For example, a list of temporarily unauthorized, or temporarily authorized usernames could be constructed (the latter could even include invalid usernames, since the account validating step 44 of the logon sequence would ensure these were not admitted), or the user number 33 could be required to be within a specified interval. The privileged user executing this program would always included."

TABLE 3B

Regarding Applicants' dependent claims 17-25 and 29, claims 17-25 and 29 are either directly or indirectly dependent upon independent claim 16. These dependent claims incorporate all the limitations of the independent claim upon which they depend while providing further unique and non-obvious recitations. Since it has been shown above that the rejection of claim 16 is not supported by the Chapman disclosure and claim 16 is not anticipated, the rejections of these dependent claims 17-25 and 29 as anticipated are also not supported by the Chapman reference and should be withdrawn. The discussion below concerns dependent claims 17-19, 25 and 29 which stand rejected as anticipated under 35 U.S.C. § 102(b). See Table 4 for a side-by-side comparison of the limitations of Applicants' claims 17-19 and 25 with the citations relied on by the Office for rejecting these claims.

Considering further Applicants' dependent claim 17, claim 17 recites the limitation, "wherein the at least one new-user identity attribute comprises a new-user profile." The Office has cited column 5, line 65 through column 6, line 3 as disclosing the limitation of claim 17. See row 1 of Table 4A for a side-by-side comparison of the limitation of claim 17 with the passage cited by the Office. Claim 17 describes the at least one new user identity attribute, described above and defined in a dictionary as any inherent characteristic or object closely associated with or belonging to a specific person, as comprising a new user profile. The profile cited by the Office describes a computer file /etc/profile used by a shell program to personalize a user's work environment in a UNIX operating system. Although the names are the same, the use of "profile" in the context of Applicants' claims and the use of "profile" in the context of the Chapman disclosure are entirely different. Contrast Applicants' use of a profile comprising at least one new user identity attribute to qualitatively identify a new user with Chapman's use of a profile to describe a UNIX operating system file for configuring a user's work environment. There is no disclosure in the Chapman reference of the limitation of Applicants' claim 17. As shown in row

1 of Table 4A, there is no correspondence between the limitation of Applicants' claim 17, and the passages in the Chapman reference cited by the Office.

Considering further Applicants' claim 18 and claim 19, claim 18 recites the limitation, "wherein the at least one database of denied-user identity attributes comprises at least one database of denied-user profiles." and claim 19 recites the limitation, "wherein the step of similarity searching comprises similarity searching the new-user profile against the at least one denied-user profile database." The Office has cited column 6, line 58 through column 7, line 6 as disclosing the limitation of claims 18 and 19. See rows 2 and 3 of Table 4A for a side-by-side comparison of the limitation of claims 18 and 19 with the passage cited by the Office. Claim 18 describes at least one database of denied user identity attributes that comprises at least one database of denied user profiles. As described above in relation to claim 17, the UNIX operating system profile files for configuring a user's work environment bear no relationship to Applicants' denied user profiles comprising denied user identity attributes that identify any inherent characteristic or object closely associated with or belonging to a specific person. Claim 19 describes similarity searching a new user profile against at least one denied user profile database. There is no disclosure in Chapman of similarity searching a new user profile against a denied user database. There is no suggesting or teaching of similarity searching in the Chapman reference, nor is there any disclosure of a denied user profile database comprising denied user identity attributes. A database of temporarily unauthorized usernames is not a denied user profile database. There is no disclosure in the Chapman reference of the limitations of Applicants' claims 18 and 19. As shown in rows 2 and 3 of Table 4A, there is no correspondence between the limitations of Applicants' claims 18 and 19, and the passages in the Chapman reference cited by the Office.

Considering Applicants' claim 25, claim 25 recites the limitation, "wherein the similarity search result comprises at least one hierarchical document stored in the at least one database of denied-user identity attributes." The Office cited column 6, line 65 through column 7, line 3 as disclosing the limitations of claim 25. See row 4 in Table 4B for a side-by-side comparison of the limitation of claim 25 with the passage cited by the Office. The passage cited by the Office in Chapman describes modifying the system-wide profile by addition of code to the system-wide profile file /etc/profile used by a shell program for defining a user's environment to log off a user if the user is temporarily unauthorized. There is no disclosure in Chapman of a similarity search result or of a hierarchical document stored in a database of denied-user identity attributed. As described above in relation to claim 17, the UNIX operating system profile files for configuring a user's work environment bear no relationship to Applicants' denied user profiles comprising denied user identity attributes that identify any inherent characteristic or object closely associated with or belonging to a specific person, as recited in claim 25. There is no disclosure in the Chapman reference of any of the limitations of Applicants' claim 25. As shown in row 4 of Table 4B, there is no correspondence between the limitations of Applicants' claim 25, and the passages in the Chapman reference cited by the Office.

Considering Applicants' claim 29, claim 29 recites the limitation, "A computer-readable medium containing instructions for controlling a computer system to implement the method of claim 16." As described above, claim 16 is not anticipated by the Chapman reference. Since claim 29 is dependent on claim 16 and incorporates all the limitations of claim 16, claim 29 is also not anticipated by the Chapman reference.

As described above, the limitations of Applicants claims 17-19, 25 and 29 are not disclosed in the Chapman reference. Therefore, claims 17-19, 25 and 29 are not anticipated under 35 U.S.C. 102(b) by the Chapman reference and should be withdrawn.

COMPARISON OF DEPENDENT CLAIMS 17-19 AND 25 LIMITATIONS WITH PASSAGES CITED BY THE OFFICE		
CLAIM LIMITATIONS	CITATION	OFFICE ASSERTED EQUIVALENT IN CHAPMAN
1. Claim 17 "wherein the at least one new-user identity attribute comprises a new-user profile."	Chapman: Column 5, Line 65 through Column 6, Line 3	The cited passage is part of a description of the UNIX logon sequence, as the title in column 5, line 12 illustrates, and is based on a conventional AIX operating system logon sequence. As described in column 4, lines 49-55, "In UNIX, a shell is a command interpreter that must be running for a user to have an interactive logon session." The citation in the Chapman reference describes "programs referred to as profiles are run 70." These programs are described as system-wide profile /etc/profile 72, and a file called profile in the user's home directory that is run subsequently by a shell program. As is well-known to UNIX operating system programmers, the profile file /etc/profile are system-wide profile files that contain initialization data used by the login shell at login time for personalizing a user's work environment by setting exported environment variables, definitions settings and terminal mode. A profile file includes at least a PATH statement and a MANPATH statement.
2. Claim 18 "wherein the at least one database of denied-user identity attributes comprises at least one database of denied-user profiles."	Chapman: Column 6, Line 58 through Column 7, Line 6	The cited passage includes a description of creating a definition of temporarily unauthorized or temporarily authorized usernames. The passage also describes the addition of code to the system-wide profile file /etc/profile used by the shell program for defining a user's environment (as described above) to log off a user if the user is temporarily unauthorized.
3. Claim 19 "wherein the step of similarity searching comprises similarity searching the new-user profile against the at least one denied-user profile database."		

TABLE 4A

COMPARISON OF DEPENDENT CLAIMS 17-19 AND 25 LIMITATIONS WITH PASSAGES CITED BY THE OFFICE		
CLAIM LIMITATIONS	CITATION	OFFICE ASSERTED EQUIVALENT IN CHAPMAN
4. Claim 25 "wherein the similarity search result comprises at least one hierarchical document stored in the at least one database of denied-user identity attributes."	Chapman: Column 6, Line 65 through Column 7, Line 3	The cited passage describes the step of modifying the system-wide profile by the addition of code to the system-wide profile file /etc/profile used by the shell program for defining a user's environment (as described above) to log off a user if the user is temporarily unauthorized.

TABLE 4B

Considering Applicants independent claim 27, the first element of Applicants' claim 27 recites the limitation, "a means for receiving at least one identity attribute from the new-user". See row 1 of Table 5A for a side-by-side comparison of this first limitation of claim 27 with the passage from the Chapman reference that the Office asserts is equivalent. Applicants contend that this claim limitation is not explicit, implicit or inherent in the passage in Chapman cited by the Office, as shown in Table 5A. The at least one identity attribute in this limitation is not constrained to be user names and passwords for gaining access to a computer system, as cited by the Office in column 1, lines 17-20 of the Chapman reference. Note that during patent examination, the pending claims must be given their broadest reasonable interpretation consistent with the specification. *In re Hyatt*, 211 F.3d 1367, 1372 (Fed. Cir. 2000). While the Chapman reference relies on usernames and passwords assigned by a system owner for authorizing access, Applicants claimed invention relies on at least one identity attribute to verify a new user identity, where the dictionary definition of attribute is any inherent characteristic or object closely associated with or belonging to a specific person. Applicants' at least one identity attribute is input by a new user prior to allowing or denying the new user access to the computer system, for determining that the new user is the person identified by the identity attribute. Since, at the time a new user enters the at least one identity attribute, the new user has not given access to the computer system, the new user has not been assigned a username and password for system access by a system owner. Applicants' at least one identity attribute is used to determine if the new user has been involved in fraudulent activities in the past, prior to allowing system access via a username and password information, as described in the Chapman reference for gaining access to a computer system. There is no disclosure in Applicants' claimed invention of supplying a username and password when the user logs on, as disclosed in the Chapman

reference. All users of a computer system must enter the access information listed in the Chapman reference every time a user wishes to gain access to the computer system. The at least one identity attribute profile data of Applicants' disclosure is only required by a new user, prior to allowing initial system access by a new user, to determine if the new user qualifies for access to the computer system. Once a new user qualifies for access to the computer system resulting from a negative similarity match according to Applicants' invention, the new user no longer needs to be re-qualified by inputting identity attribute profile data. Once a new user has been qualified by a negative similarity match and allowed to gain access to the computer system, the new user is no longer a new user, and becomes a normally authorized user as disclosed in the Chapman reference. Therefore, when the meaning of this first limitation of Applicants' claim 27, namely, "a means for receiving at least one identity attribute from the new-user" is given it broadest reasonable interpretation, this limitation is not found in the Chapman reference cited by the Office, because the new user has not been assigned a user name and password by a system owner. As shown in row 1 of Table 5A, there is no correspondence between the limitation of the first element of Applicants' claim 27, and the passages in the Brown reference cited by the Office.

The second and third element of Applicants' claim 27 recite the limitation, "at least one database for storing denied-user identity attributes" and "at least one database for storing valid user identities", respectively. The Chapman reference includes the disclosure of authorized usernames, temporarily authorized usernames and temporarily unauthorized usernames. However, there is no disclosure in the Chapman reference of a database for storing denied user identity attributes and a database for storing valid user identities.

The fourth element of Applicants' claim 27 recite the limitation, "a means for similarity

searching the at least one new user identity attribute against at least one database of denied user attributes". As described above, U.S. Patent No. 6,618,727, which is incorporated herein by reference, discloses a similarity search engine that may be used for similarity searching by comparing two documents to determine an indicia of similarity that provides a quantitative measure of how alike the two documents are, such as new user identity attributes and denied user identity attributes. This similarity search engine is used to similarity search the identity attributes against denied user identity attributes and provide a similarity search result that includes indicia of similarity. The denied user identity attributes contain identity attributes of users that have been removed or suspended from the system in the past. If a new user identity attribute has a positive similarity match to a suspended-user's identity attributes, the new user is denied access to the computer system. There is no disclosure of these limitations in the Chapman reference.

The fifth and sixth element of Applicants' claim 27 recite the limitations "a means for determining a positive or negative similarity match between at least one new user attribute and the at least one database of denied user identity attributes" and "a means for allowing the new user to access the computer system, where a negative similarity match has been determined", respectively. There is no disclosure in the Chapman reference of determining a positive or negative similarity match between identity attribute profile data and suspended-users identity attribute profile data based on the similarity search result. There is also no disclosure in the Chapman reference of allowing a new user access to the system where a negative similarity match has been determined. The Chapman reference discloses validating a user account by (positively) matching a supplied user name with a username in a valid account, and authenticating the user by comparing the true password corresponding to the validated username with a password supplied by the user who is attempting to gain access.

The seventh element of Applicants' claim 27 recites the limitation, "a means for denying the new-user access to the computer system, where a positive similarity match has been determined". There is no disclosure in the Chapman reference of denying user access based on a positive similarity match. The Chapman reference discloses temporarily restricting access to the system using user privileged status and profile file.

The Office cites column 6, line 58-63 of the Chapman reference as disclosing Applicants' second through seventh limitations of claim 16. See rows 2-7 of Table 5A for a side-by-side comparison of the second through seventh limitation of claim 27 with the passage from the Chapman reference that the Office asserts is equivalent. Applicants contend that this claim limitation is not explicit, implicit or inherent in the passage in Chapman cited by the Office, as shown in Table 5A. This passage describes conventional methods for validating a user account by exact matching of usernames or user numbers provided by a user during a login sequence with data stored in a database file containing unauthorized or temporarily authorized user names or user numbers. Access to the computer system by a user is authenticated by exact comparison of the encrypted true password with that supplied by a user attempting to logon, and establishing exact user credentials stored in a database. This cited passage requires positive exact matching of usernames and passwords for allowing access, which may be performed by conventional database management systems. Where a positive exact match is found, a user is allowed access to the computer system. Whereas, with Applicants' claimed invention, when a positive similarity match between the at least one new user identity attribute and a denied user identity attributes is determined, access by the new user is denied. There is no disclosure of similarity searching as disclosed by Applicants in this cited passage, and furthermore, a similarity search would not be applicable or desirable to this application, since persons other than an authenticated user may

gain access to the computer system by providing similar usernames and passwords. There is also no disclosure in the Chapman reference of similarity searching identity attribute profile data against denied-users identity attribute profile data. There is no disclosure of either similarity searching or of denied-users identity profile data in the Chapman reference, which merely describes authorized users, temporarily unauthorized users, temporarily authorized users and a privileged user for controlling the authorization and unauthorization process. There is no disclosure in the cited passage in the Chapman reference of receiving a similarity search result. Furthermore, in order to accomplish this limitation, a similarity search engine like that disclosed in U.S. Patent No. 6,618,727 would be required. As shown in rows 2-7 of Table 5A, there is no correspondence between the limitations of Applicants' claim 27, and the passages in the Chapman reference cited by the Office.

The Office also cited column 4, lines 13-22 and column 6, lines 23-25 as disclosing the second through seventh limitations of claim 27. See rows 2-7 in Table 5A for a side-by-side comparison of the limitation of claim 27 with the passages cited by the Office. The passage cited by the Office in column 4, lines 13-22 of Chapman describe creating a user account for enabling system access and a user's home directory for storing user programs and data. There is no relationship between this Chapman citation for creating a new user account and Applicants' adding a new user identity to at least one database of valid user identities, where a negative similarity match has been determined. The passage cited by the Office in column 6, lines 23-25 of Chapman describe temporarily restricting access to a system by determining if the user of the access control program is privileged. There is no relationship between a check to determine if the user of the access control program is privileged, as recited in Chapman, and adding a new user identity to at least one database of valid user identities where a negative similarity match has

been determined, as recited in Applicants' claim 27. As shown in rows 2-7 of Table 5A, there is no correspondence between the limitations of Applicants' claim 27, and the passages in the Chapman reference cited by the Office.

Considering the eighth limitation of Applicants' claim 27, shown in row 8 of Table 5B, the Office has cited the passage in Chapman at column 4, lines 13-22 as adding a new user to a valid user identity database where a negative similarity match has been determined. The passage cited by the Office in column 4, lines 13-22 of Chapman describe creating a user account for enabling system access and a user's home directory for storing user programs and data. There is no relationship between this Chapman citation for creating a new user account and Applicants' adding a new user identity to at least one database of valid user identities, where a negative similarity match has been determined. As shown in row 8 of Table 5B, there is no correspondence between the limitations of Applicants' claim 27, and the passages in the Chapman reference cited by the Office.

The Office also cited column 6, lines 56-64 as disclosing the ninth limitation of claim 27. See row 9 in Table 5B for a side-by-side comparison of this limitation of claim 27 with the passage cited by the Office. The passage cite by the Office in column 6, lines 56-64 of Chapman describe creating a definition of temporarily unauthorized users. There is no relationship between creating a definition of temporarily unauthorized users, as recited in Chapman, and the limitation of denying the new user access to the computer system and adding new user identity attributes to the at least one database of denied user attributes where a positive similarity match has been determined, as recited in Applicants' ninth limitation of claim 27. There is no disclosure in the Chapman reference of any of the limitations of Applicants' claim 27. As shown in row 9 of Table 5B, there is no correspondence between the limitations of Applicants' claim 27, and the

passages in the Chapman reference cited by the Office.

It should be especially noted that for conventional applications involving authenticating usernames and passwords for computer access, exact matching of these parameters is a requirement every time a user desires access to the system. In contrast, when attempting to uncover computer access through fraudulent means, non-exact or similarity matching is desirable in order to make a determination of fraudulent activity based on degrees of similarity on a one time basis for new users.

Since every element of Applicants' claimed invention, arranged as in independent claim 27, are not found implicitly, explicitly or inherently in the single reference of Chapman, the Office has failed to substantiate a *prima facie* case for anticipation and Chapman et al does not anticipate Applicants' independent claim 27. Therefore the rejection of claim 27 should be withdrawn.

COMPARISON OF CLAIM 27 LIMITATIONS WITH PASSAGES CITED BY THE OFFICE		
CLAIM LIMITATIONS	CITATION	OFFICE ASSERTED EQUIVALENT IN CHAPMAN
1. "a means for receiving at least one identity attribute from the new user"	Chapman: Column 1, Lines 17-20	"In most multiuser systems, a file or files listing valid usernames, or valid combinations of usernames and passwords are kept, and a user gains access to the system by supplying such a name and password when he logs on."
2. "at least one database for storing denied-user identity attributes" 3. at least one database for storing valid user identities; 4. "a means for similarity searching the at least one new-user identity attribute against at least one database of denied-user attributes" 5. "a means for determining a positive or negative similarity match between the at least one new-user attribute and the at least one database of denied-user identity attributes" 6. "a means for allowing the new-user to access the computer system, where a negative similarity match has been determined" 7. "a means for denying the new-user access to the computer system, where a positive similarity match has been determined	Chapman: Column 6, Lines 58-63	"For example, a list of temporarily unauthorized, or temporarily authorized usernames could be constructed (the latter could even include invalid usernames, since the account validating step 44 of the logon sequence would ensure these were not admitted), or the user number 33 could be required to be within a specified interval."
	Chapman: Column 4, Line 13-22	The cited passage describes adding a new user to a UNIX system by creating a "user account" consisting of two parts: an entry for enabling system access in a file entitled /etc/password that defines accounts and their characteristics; and a user's home directory for storing user programs and data.
	Chapman: Column 6, Line 23-25	The cited passage describes a method for temporarily restricting access to a system that comprises a check to determine if the user of the access control program is privileged. In UNIX terms, the privileged user must have superuser authority, such as the system owner.

TABLE 5A

COMPARISON OF CLAIM 27 LIMITATIONS WITH PASSAGES CITED BY THE OFFICE		
CLAIM LIMITATIONS	CITATION	OFFICE ASSERTED EQUIVALENT IN CHAPMAN
8. "a means for adding the new-user identity to the at least one database for storing valid user identities, where a negative similarity match has been determined"	Chapman: Column 4, Lines 13-22	The cited passage describes adding a new user to a UNIX system by creating a "user account" consisting of two parts: an entry for enabling system access in a file entitled /etc/password that defines accounts and their characteristics; and a user's home directory for storing user programs and data.
9. "a means for adding the at least one new-user identity attribute to the at least one database of denied-user attributes, where a positive similarity match has been determined"	Chapman: Column 6, Lines 56-64	"Check (users to be permitted access) and create 89 a definition of temporarily unauthorized users, by any appropriate method. For example, a list of temporarily unauthorized, or temporarily authorized usernames could be constructed (the latter could even include invalid usernames, since the account validating step 44 of the logon sequence would ensure these were not admitted), or the user number 33 could be required to be within a specified interval. The privileged user executing this program would always included."

TABLE 5B

Response to Claim Rejections Under 35 U.S.C. §103(a)

The Office has rejected claims 5-11, 20-23, 30 and 31 under 35 U.S.C. § 103(a) as being unpatentable over Chapman et al. (U.S. Patent No. 5,774,650) in view of U.S. Patent No. 6,026,398 to Brown et al. The Office bears the initial burden of establishing a *prima facie* case of obviousness. *See In re Piasecki*, 223 USPQ785, 788 (Fed. Cir. 1984). To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *In re Vaeck*, 20 USPQ2d 1438 (Fed. Cir. 1991), MPEP § 2142 and § 2143.

Regarding Applicants' dependent claims 5-11 and claims 20-23, claims 5-11 are either directly or indirectly dependent upon independent claim 1 and claims 20-23 are either directly or indirectly dependent upon independent claim 16. These dependent claims incorporate all the limitations of the independent claim upon which they depend while providing further unique and non-obvious recitations. Since it has been shown above that the rejections of claims 1 and 16 are not supported by the Chapman disclosure and therefore are not anticipated, the rejections of these dependent claims 5-11 and 20-23 as obvious are also not supported by the Chapman reference and should be withdrawn.

Considering further Applicants' claims 5 and 20, claims 5 and 20 recite the limitation, "wherein the step of determining a positive or negative similarity match further comprises

comparing the similarity search result to a first match tolerance level." See row 1 of Table 6A for a side-by-side comparison of the limitations of claims 5 and 20 with the passages from the Brown reference that the Office asserts is equivalent. As described above, U.S. Patent No. 6,618,727, which is incorporated herein by reference, discloses a similarity search engine that may be used for similarity searching by comparing two documents to determine indicia of similarity that provides a quantitative measure of how alike the two documents are, such as a new user profile data and suspended-users profile data. This similarity search engine is used to similarity search the profile data against suspended-users profile data and provide a similarity search result set that includes indicia of similarity. The Office cites column 13, lines 1-4 of Brown as comparing the result to a weight and column 13, lines 21-26 of Brown as determining an accurate match and to determine how close is the match. There is no disclosure in these citations or anywhere in either the Chapman and Brown reference of determining a positive or negative similarity match, or of comparing a similarity search result to a first match tolerance level. There is no disclosure of a similarity search function, as disclosed in Applicants' specification, in the Brown reference. Brown discloses using a Soundex function to convert elements of input search data to terms having a finite set of possible values, and using statistical analysis to weight records to calculate how close input data is to each match record. This disclosure in the Brown reference does not disclose determining a positive or negative similarity match by comparing the similarity search result to a first match tolerance level that the limitation of Applicants' claims 5 and 20 recite. As shown in row 1 of Table 6A, there is no correspondence between the limitations of Applicants' claims 5 and 20, and the passages in the Brown reference cited by the Office.

Considering Applicants' claims 6 and 21, claims 6 and 21 a recite the limitation "wherein a positive similarity match comprises a similarity match, between the at least one new-user identity attribute and at least one denied-user identity attribute, that meets or exceeds the first match tolerance level" and claims 7 and 22 recite the limitation "wherein a negative similarity match comprises a similarity match, between the at least one new-user identity attribute and at least one denied-user identity attribute, that does not meet or exceed the first match tolerance level." See rows 2 and 3 of Table 6A for a side-by-side comparison of Applicants' claims 6, 7, 21 and 22 with the passages from the Brown reference that the Office asserts is equivalent. The cited passage in Brown at column 13, lines 27-30 describes data the is somewhat "close" to input search data, and the cited passage in Brown at 13, lines 21-26 describes determining an accurate match and to determine how close is the match. There is no disclosure in these citations or anywhere in either the Chapman or Brown reference of determining a positive or negative similarity match between the at least one new user identity attribute and the at least one denied user identity attribute that meets or exceeds the first match tolerance level, or that does not meet or exceed the first match tolerance level that the limitations of Applicants' claims 6, 7, 21 and 22 recite. As shown in rows 2 and 3 of Table 6A, there is no correspondence between the limitations of Applicants' claims 6, 7, 21 and 22, and the passages in the Brown reference cited by the Office.

Considering Applicants' claim 8, claim 8 recites "where a positive similarity match has been determined, verifying the positive similarity match via a secondary review, after the step of determining whether a positive or negative similarity match exists and before the step of denying the new-user access to the computer system." See row 4 of Table 6B for a side-by-side comparison of the limitation of claim 8 with the passages from the Brown reference that the

Office asserts is equivalent. The cited passage in Brown at column 14, lines 8-14 describe a second function, comprising 22 record match tests, for determining if one or a few of the top ten weighted match records may be considered to be a match to the input search data. The cited passage in Brown at column 14, lines 17-21 describe a process to determine the statistical likelihood of a record corresponding to input search data. There is no disclosure in the Chapman or Brown reference of verifying a positive similarity match where a positive similarity match has been previously determined, as recited in Applicants' claim 8. As shown in row 4 of Table 6B, there is no correspondence between the limitations of Applicants' claim 8, and the passages in the Brown reference cited by the Office.

Considering Applicants' claims 9 and 23, claims 9 and 23 recite, "wherein the step of verifying the positive similarity match further comprises comparing the similarity search result to a second match tolerance level." See row 5 of Table 6B for a side-by-side comparison of the limitations of claims 9 and 23 with the passages from the Brown reference that the Office asserts is equivalent. The cited passage in Brown at column 14, lines 14-17 describe 22 tests for comparing record weights of certain match records based on statistical criteria. The cited passage in Brown at column 14, lines 17-21 describe a process to determine the statistical likelihood of a record corresponding to input search data. There is no disclosure in the Chapman or Brown reference of verifying a positive similarity match by comparing similarity search results to a second match tolerance level, as recited in Applicants' claims 9 and 23. As shown in row 5 of Table 6B, there is no correspondence between the limitations of Applicants' claims 9 and 23, and the passages in the Brown reference cited by the Office.

Considering Applicants' claims 10 and 11, claim 10 recites, "allowing the new-user to access the computer system, where the positive similarity match does not meet or exceed the

second match tolerance level" and claim 11 recites "denying the new-user access to the computer system, where the positive similarity match meets or exceeds the second match tolerance level." See rows 6 and 7 of Table 6C for a side-by-side comparison of the limitations of claims 10 and 11 with the passages from the Brown reference that the Office asserts is equivalent. The cited passage in Brown at column 14, lines 23-32 describe using only the top ten match records for 22 second function tests for producing test weights that have a zero value if a test fails and a value of K_n*W_n if the test passes. The cited passage in Brown at column 14, lines 43-47 describe three types of match conditions, whereby a hit, miss or multiple value will be assigned to the corresponding match record. There is no disclosure in the Brown or Chapman reference of allowing user access where a positive similarity match does not meet or exceed a second match tolerance level, or denying a user access where a positive similarity match meets or exceeds a second match tolerance level, as recited in Applicants' claims 10 and 11. As shown in rows 6 and 7 of Table 6C, there is no correspondence between the limitations of Applicants' claims 10 and 11, and the passages in the Brown reference cited by the Office.

COMPARISON OF DEPENDENT CLAIMS 5-11 AND 20-23 LIMITATIONS WITH PASSAGES CITED BY THE OFFICE		
CLAIM LIMITATIONS	CITATION	OFFICE ASSERTED EQUIVALENT IN BROWN
1. Claims 5 and 20 "wherein the step of determining a positive or negative similarity match further comprises comparing the similarity search result to a first match tolerance level"	Brown: Column 13, Lines 1-4	"Record weights, such as those shown in table 107, are computed by step 36 in FIG. 7 for every unique match record identifier in the several matching term sets. Table 107 only shows ten examples of computed record weights."
	Brown: Column 13, Lines 21-26	"As shown above, database records which contain data that closely matches a particular set of input search data elements will be given a record weight indicating such a close relationship due to the number of terms which match and the significance of those terms as determined by the term set weights."
2. Claims 6 and 21 "wherein a positive similarity match comprises a similarity match, between the at least one new-user identity attribute and at least one denied-user identity attribute, that meets or exceeds the first match tolerance level" 3. Claims 7 and 22 "wherein a negative similarity match comprises a similarity match, between the at least one new-user identity attribute and at least one denied-user identity attribute, that does not meet or exceed the first match tolerance level"	Brown: Column 13, Lines 27-30	"As indicated by a record weight of 16, database record number 1234 contains data that is somewhat "close" to the input search data, but not as close as record number 5873, having the highest record weight of 28, as shown in FIG. 10."
	Brown: Column 13, Lines 21-26	"As shown above, database records which contain data that closely matches a particular set of input search data elements will be given a record weight indicating such a close relationship due to the number of terms which match and the significance of those terms as determined by the term set weights."

TABLE 6A

COMPARISON OF DEPENDENT CLAIMS 5-11 AND 20-23 LIMITATIONS WITH PASSAGES CITED BY THE OFFICE		
CLAIM LIMITATIONS	CITATION	OFFICE ASSERTED EQUIVALENT IN BROWN
4. Claim 8 "further comprising, where a positive similarity match has been determined, verifying the positive similarity match via a secondary review, after the step of determining whether a positive or negative similarity match exists and before the step of denying the new-user access to the computer system."	Brown: Column 14, Lines 8-14	"As shown in FIG 11, the second function is comprised of twenty-two record match tests T1-T22 which are applied to the ten highest record weights of match records. The objective of the second function is to determine, if possible, whether one or a few of the top ten weighted match records is sufficiently distinct in its weight to be considered a match to the input search data."
	Brown: Column 14, Lines 17-21	"Each record match test outputs a test weight value which may be used in combination with other test weight values to determine the statistical likelihood of a particular match record corresponding to the input search data."
5. Claims 9 and 23 "wherein the step of verifying the positive similarity match further comprises comparing the similarity search result to a second match tolerance level"	Brown: Column 14, Lines 14-17	"Each of the twenty two tests &1-T22 in FIG. 11 manipulates and/or compares one or more of the record weights of certain match records based on statistical criteria."
	Brown: Column 14, Lines 17-21	"Each record match test outputs a test weight value which may be used in combination with other test weight values to determine the statistical likelihood of a particular match record corresponding to the input search data."

TABLE 6B

COMPARISON OF DEPENDENT CLAIMS 5-11 AND 20-23 LIMITATIONS WITH PASSAGES CITED BY THE OFFICE		
CLAIM LIMITATIONS	CITATION	OFFICE ASSERTED EQUIVALENT IN BROWN
6. Claim 10 "further comprising allowing the new-user to access the computer system, where the positive similarity match does not meet or exceed the second match tolerance level. 7. Claim 11 "further comprising denying the new-user access to the computer system, where the positive similarity match meets or exceeds the second match tolerance level	Brown: Column 14, Lines 23-32	"In each test T1-T22 shown in FIG. 11, C_n is the record weight of an n-th match record in the ranked list of record weights, shown by the table 107 in FIG. 10 of the example. Since only the top ten match records will be used for the second function tests T1-T22, n ranges from 0 to 9. As shown in FIG. 11, each test operates on certain values, and produces a test weight value W_n depending upon the outcome of the test. Test weight value W_n is a weight associated with an output of the n-th test with a value of 0 if a test fails, or a value of K_n * (times) W_n if the test passes."
	Brown: Column 14, Lines 43-47	"There are three types of match conditions which may be determined from the record match tests T1-T22 in FIG. 11. For each record weight passed through tests T1-T22 of FIG. 11, a hit, miss or multiple value will be assigned to the corresponding match record."

TABLE 6C

Regarding Applicants' independent claim 30, claim 30 recites a method for verifying the identities of new users of a computer system using similarity searching to detect identity fraud, as contrasted to the Chapman reference which discloses a method for controlling access to a networked computer system by usernames and passwords. The Brown reference discloses a system and method for searching and matching databases using Soundex functions and statistical analysis techniques, which is not similarity searching according to Applicants' specification. Applicants' similarity searching is a deterministic technique while the Brown reference discloses a probabilistic technique. These differences account for the Applicants' claim limitations that are not found in the Chapman and Brown references. See Table 7 for a side-by-side comparison of the limitations of Applicants' claims 30 with the citations relied on by the Office for rejecting Applicants' claims 30.

The first element of Applicants' claim 30 recites the limitation, "similarity searching one or more new user identity attribute profile data records against denied-user identity attribute profile data records". The Office has cited column 5, lines 30-49 and column 5, lines 57-64 of the Chapman reference as disclosing this limitation. See row 1 of Table 7A for a side-by-side comparison of the first limitation of claim 30 with this passages from the Chapman reference that the Office asserts is equivalent. Applicants contend that this claim limitation is not explicit, implicit or inherent in the passage in Chapman cited by the Office, as shown in Table 7A. The cited passage describes conventional methods for validating a user account by exact matching of usernames with those stored in a database file, authenticating the user by exact comparison of the encrypted true password with that supplied by a user attempting to logon, and establishing exact user credentials stored in a database. This is to provide a determination of whether to grant access to the system by a user. The cited passage in Chapman requires exact matching of usernames and passwords, which may be performed by conventional database management

systems. There is no disclosure of similarity searching in this cited passage, and furthermore, a similarity search would not be applicable or desirable to this application, since persons other than an authenticated user may gain access to the computer system by providing similar usernames and passwords. There is no correspondence or equivalence between Applicants' first limitation of claim 30 and the passage in Chapman cited by the Office. There is no disclosure in the Chapman reference of similarity searching profile data against suspended-users profile data. There is no disclosure of either similarity searching or of suspended-users profile data in the Chapman reference. As shown in row 1 of Table 7A, there is no correspondence between the first limitation of Applicants' claim 30, and the passages in the Chapman reference cited by the Office.

The second element of Applicants' claim 30 recites the limitation, "receiving one or more similarity search results sets, each result set having a corresponding new user identity attribute profile data record and a corresponding similarity match score". The Office has cited column 3, line 66 through column 4, line 7 of the Brown reference as disclosing this limitation. See row 2 of Table 7A for a side-by-side comparison of the second limitation of claim 30 with this passage from the Brown reference that the Office asserts is equivalent. Applicants contend that this claim limitation is not explicit, implicit or inherent in the passage in Brown cited by the Office, as shown in Table 7A. The cited passage discloses reliance on the matching index entries using a Soundex function that phonetically encodes text elements for computing record weights and determining match conditions for indicating how close input data is to certain match records using a second function described in Column 4, Lines 8-15 as a statistical test. There is no disclosure in this passage of receiving similarity search result sets having a corresponding new user identity attribute profile and a corresponding similarity match score, as in Applicants' claim 30 and disclosed in U.S. Patent No. 6,618,727. The passage cited by the Office does not disclose

the second limitation of Applicants' claim 30. As shown in row 2 of Table 7A, there is no correspondence between the second limitation of Applicants' claim 30, and the passages in the Brown reference cited by the Office.

The third element of Applicants' claim 30 recites the limitation, "comparing each similarity match score with a pre-determined match tolerance level for determining negative similarity match scores and positive similarity match scores". The Office has cited column 14, lines 49-51 of Brown as disclosing this limitation. See row 3 of Table 7B for a side-by-side comparison of the third limitation of claim 30 with this passage from the Brown reference that the Office asserts is equivalent. Applicants contend that this claim limitation is not explicit, implicit or inherent in the passage in Chapman cited by the Office, as shown in Table 7B. The cited passage discloses multiple match conditions when more than one match record matches input search data above a threshold amount. There is no disclosure of comparing the match score with a pre-determined match tolerance level for determining negative and positive similarity match scores, as illustrated in row 3 of Table 7B. The passages cited by the Office do not disclose the third limitation of Applicants' claim 30.

Considering the fourth and fifth elements of Applicants' claim 30, the fourth element of Applicants' claim 30 recites the limitation, "for each negative similarity match score having a value of less than or equal to the pre-determined match tolerance level, allowing access to the computer system by a new user associated with a new user identity attribute profile data record corresponding to a negative similarity match score". The fifth element of Applicants claim 30 recites the limitation "for each positive similarity match score having a value greater than the pre-determined match tolerance level, denying access to the computer system by a new user associated with a new user identity attribute profile data record corresponding to a positive similarity match score". The Office has cited column 4, lines 27-30 of Brown as disclosing the

fourth and fifth limitations of Applicants' claim 30. See rows 4 and 5 of Table 7B for a side-by-side comparison of the fourth and fifth limitations of claim 30 with this passage from the Brown reference that the Office asserts is equivalent. Applicants contend that these claim limitations are not explicit, implicit or inherent in the passage in Brown cited by the Office, as shown in Table 7B. The cited passage of column 4, lines 27-30 of Brown describes a Q-Gram function that allows the invention to determine a precise match condition. There is no disclosure in Applicants' specification of a G-Gram function. There is no disclosure in the passage cited by the Office of positive and negative similarity match scores, predetermined match tolerance levels, and new user identity attribute profile data. The passage cited by the Office does not disclose the fourth and fifth limitation of Applicants' claim 30. As shown in rows 4 and 5 of Table 7B, there is no correspondence between the fourth and fifth limitations of Applicants' claim 30, and the passages in the Brown reference cited by the Office.

Since every element of Applicants' claimed invention, arranged as in the independent claim 30, is not found implicitly, explicitly or inherently in Chapman in view of Brown, the Office has failed to substantiate a *prima facie* case for obviousness for Applicants' independent claim 30. Therefore the rejection of claim 30 should be withdrawn. Furthermore, claim 31 is either directly dependent upon independent claim 30. This dependent claim incorporates all the limitations of the independent claim upon which it depends while providing further unique and non-obvious recitations. Since the rejection of claim 30 is not supported by the Chapman and Brown disclosures, the rejections of dependent claim 31as obvious is also not supported by the Chapman and Brown references and should be withdrawn. Applicants request withdrawal of the rejection of claims 30 and 31, reconsideration and reexamination of the application.

COMPARISON OF INDEPENDENT CLAIM 30 LIMITATIONS WITH PASSAGES CITED BY THE OFFICE		
CLAIM LIMITATIONS	CITATION	OFFICE ASSERTED EQUIVALENT IN CHAPMAN AND BROWN
1. "similarity searching one or more new user identity attribute profile data records against denied-user identity attribute profile data records"	Chapman: Column 5, Lines 30-49	Describes a process of checking a user account details 42 at logon, as shown in Figure 3 of Chapman. The step 42 comprises the steps of validating 44, authenticating 46 and establishing credentials 48. Validating 44 the user account is performed by checking that a username 31 exists in a file 30 that matches the username supplied by the user attempting to gain access. Authenticating 46 the user is performed by comparing an encrypted true password 31 with an encrypted password supplied by the user attempting to gain access. Establishing credentials 48 is data stored in a database that define the user's accountability and access rights to files on the system. The step 42 of checking account details is the step at which it is normally determined whether or not a user is to be granted access to the system 2 and allowed to proceed with the later steps in the logon sequence.
	Chapman: Column 5, Lines 57-64	After initializing the user environment, the user is placed in a directory specified by a UNIX password file as his home directory and the initial program is a shell program that provides a command line interface.
2. "receiving one or more similarity search results sets, each result set having a corresponding new user identity attribute profile data record and a corresponding similarity match score"	Brown: Column 3, Line 66 through Column 4, Line 7	The cited passage relies on a first function described in Column 3, Lines 47-65 to determine matching index entries. This function is described as a Soundex function that phonetically encodes text elements. The cited passage discloses reliance on the matching index entries using a Soundex function for computing record weights and determining match conditions for indicating how close input data is to certain match records using a second function described in Column 4, Lines 8-15 as a statistical test.

TABLE 7A

COMPARISON OF INDEPENDENT CLAIM 30 LIMITATIONS WITH PASSAGES CITED BY THE OFFICE		
CLAIM LIMITATIONS	CITATION	OFFICE ASSERTED EQUIVALENT IN CHAPMAN AND BROWN
3. "comparing each similarity match score with a pre-determined match tolerance level for determining negative similarity match scores and positive similarity match scores"	Brown: Column 14, Lines 49-51	"A multiple match condition exists when one or more match record matches the input search data above a predetermined threshold amount."
4. "for each negative similarity match score having a value of less than or equal to the pre-determined match tolerance level, allowing access to the computer system by a new user associated with a new user identity attribute profile data record corresponding to a negative similarity match score" 5. "for each positive similarity match score having a value greater than the pre-determined match tolerance level, denying access to the computer system by a new user associated with a new user identity attribute profile data record corresponding to a positive similarity match score	Brown: Column 4, Lines 27-30	"The Q-gram function allows the invention to exactly determine a precise match condition for the closest database match records."

TABLE 7B

Considering the first element of Applicants' dependent claim 31, the first element of claim 31 recites the limitation "confirming whether the positive similarity match score exists between the new user identity attribute profile data record and a corresponding suspended-users identity attribute profile data record." The Office cites column 13, lines 49-59 of Brown as disclosing whether a positive similarity match score exists between the new user identity attribute profile data record and a corresponding suspended users identity attribute profile data record. See row 1 of Table 8 for a side-by-side comparison of this limitation of claim 31 with this passage from the Brown reference that the Office asserts is equivalent. Applicants contend that this claim limitation is not explicit, implicit or inherent in the passage in Brown cited by the Office, as shown in Table 8. The cited passage of column 13, lines 49-59 of Brown describes a process for determining a likelihood of a close match between individual match records and input search data using Soundex functions and statistical analysis functions. There is no disclosure in Applicants' specification of the use of Soundex functions or statistical analysis functions for determining a match between input search data and match records. There is no disclosure in the Brown reference of a similarity search function providing similarity match scores. There is no disclosure of determining whether a positive similarity match score exists between the new user profile data record and a corresponding suspended users profile data record, as illustrated in row 1 of Table 8.

Considering the second and third element of Applicants' dependent claim 31, the third element recites the limitation, "allowing a new user associated with a new user identity attribute profile data record corresponding to a positive similarity match score to access the computer system, where the positive similarity match score is not confirmed", and the fourth element recites the limitation, "denying a new user associated with a new user identity attribute profile

data record corresponding to a positive similarity match score access to the computer system, where the positive similarity match score is confirmed". The Office cites column 13, lines 55-59 of Brown as disclosing allowing or denying a user access to the computer system where the positive similarity match score is not confirmed or confirmed, respectively. See rows 2 and 3 of Table 8 for a side-by-side comparison of the second and third limitations of claim 31 with this passage from the Brown reference that the Office asserts is equivalent. Applicants contend that this claim limitation is not explicit, implicit or inherent in the passage in Brown cited by the Office, as shown in Table 8. The cited passage of column 13, lines 55-59 of Brown describes a step that uses statistical analysis functions in the process for determining a likelihood of a close match between individual match records and input search data using Soundex functions and statistical analysis functions. There is no disclosure in Applicants' specification of the use of Soundex functions or statistical analysis functions for determining a match between input search data and match records. There is no disclosure in the Brown reference of a similarity search function for providing positive similarity match scores. There is no disclosure for allowing a user access to the computer system where the positive similarity match score is not confirmed, or of denying a user access to the computer system where the positive similarity match score is confirmed, as illustrated in rows 2 and 3 of Table 8.

Since every element of Applicants' claimed invention, arranged as in dependent claim 31, is not found implicitly, explicitly or inherently in Chapman in view of Brown, the Office has failed to substantiate a *prima facie* case for obviousness for Applicants' dependent claim 31. Therefore the rejection of claim 31 should be withdrawn.

COMPARISON OF DEPENDENT CLAIM 31 LIMITATIONS WITH PASSAGES CITED BY THE OFFICE		
CLAIM LIMITATIONS	CITATION	OFFICE ASSERTED EQUIVALENT IN BROWN
1. "confirming whether the positive similarity match score exists between the new user identity attribute profile data record and a corresponding suspended-users identity attribute profile data record"	Brown: Column 13, Lines 49-59	In the description of Figure 7 for determining match records, after the step of 35 determining a set of match records using Soundex functions, the step of 36 computing record weight of match records, the step of 37 includes receiving the entire set of match records with the record weights and applying a second statistical analysis function for determining a likelihood of a close match between individual match records and the input search data.
2. "allowing a new user associated with a new user identity attribute profile data record corresponding to a positive similarity match score to access the computer system, where the positive similarity match score is not confirmed" 3. "denying a new user associated with a new user identity attribute profile data record corresponding to a positive similarity match score access to the computer system, where the positive similarity match score is confirmed"	Brown: Column 13, Lines 55-59	"Generally, the second function may be any statistical analysis function which compares the record weights of each unique match record, or a subset thereof, and determines the likelihood of a close match between individual match records and the input search data."

TABLE 8

The Office has also rejected claims 13 and 24 under 35 U.S.C. § 103(a) as being unpatentable over Chapman et al. (U.S. Patent No. 5,774,650) in view of U.S. Patent No. 6,626,092 to Berke. Claim 13 is dependent upon independent claim 1 and claim 24 is dependent on independent claim 16. These dependent claims incorporate all the limitations of the independent claim upon which they depend while providing further unique and non-obvious recitations. Since it has been shown above that the rejection of claims 1 and 16 are not supported by the Chapman disclosure and are not anticipated, the rejections of these dependent claims 13 and 24 as obvious are also not supported by the Chapman reference and should be withdrawn.

Since the references of Chapman, Brown and Berke cited by the Office do not teach or suggest every element of Applicants' claimed invention, arranged as in the claims 5-11, 13, 20-24, 30 and 31, the Office has failed to substantiate a *prima facie* case for obviousness under 35 U.S.C. § 103(a). Therefore the rejection of claims 5-11, 13, 20-24, 30 and 31 are not supported by the cited references, and should be withdrawn. Applicants request withdrawal of the rejection of these claims, reconsideration and reexamination of the application.

Applicants' Answer to Office Comments Concerning Applicants' Prior Arguments

In the second Office Action of June 21, 2005, the Office responded to Applicants arguments presented in response to the first Office Action with the following allegations.

1. The Office alleges "similarity matching are not recited in the rejected claims". Applicant respectfully requests that the Office read the claims again. For example, Applicants' independent claim 1 recites "similarity searching", "similarity search result", "determining a positive or negative similarity match...based on the similarity search result", "allowing the new user access...where a negative similarity match has been determined", and "denying the new user access...where a positive similarity match has been determined. These recitations are also found in Applicants' independent claims 16, 27 and 30, as well as in many of the dependent claims. "Similarity matching" and supporting features are clearly recited in Applicants' claims.

2. Regarding Applicants' claims 1, 16 and 27, the Office alleges that identity attribute used to determine if the new user has been involved in fraudulent activities is disclosed in Chapmen at column 1, lines 21-38. Applicants can find no disclosure of new users, identity attributes or fraudulent activities in the cited passage, as in Applicants' claims.

Regarding Applicants' claims 1, 16 and 27, the Office alleges that new user attribute information is disclosed as being entered only once in the Chapman reference at column 4, lines 16-26, through the use of the AIX operating system file etc/passwd. The cited passage in Chapman describes the etc/passwd file as defining user accounts and their characteristics, not identity attributes of new users as claimed by Applicants. There is no disclosure in the cited passage of Chapman of entering new user attribute information only once.

Regarding Applicants' claims 1, 16 and 27, the Office alleges that denied user identity profile data, and positive and negative similarity matches are disclosed in the Chapman reference in column 6, lines 58-64 and column 5, line 30-41. The cited passages describes use temporarily unauthorized and authorized usernames in a validating step of a logon sequence, and verifying a user identity by matching account usernames and passwords with a username and password of a user attempting to gain access to the system. There is no disclosure of denied user identity profile data, and positive and negative similarity matches, as claimed by Applicants, in the cited passages by the Office.

Regarding Applicants' claims 1, 16 and 27, the Office alleges that determining a positive or negative similarity match between at least one new user identity attribute and the denied user identity attributes based on similarity search results, allowing access for a negative match and denying access for a positive match, as claimed by Applicants, is disclosed in Chapman in column 6, line 56 through column 7, line 6. The passage cited by the Office includes a description of creating a definition of temporarily unauthorized or temporarily authorized usernames. The passage also describes the addition of code to the system-wide profile file

/etc/profile used by the shell program for defining a user's environment (as described above) to log off a user if the user is temporarily unauthorized. The profile file /etc/profile is a standard UNIX operating system file that defines a user work environment on a system, and does not provide new user identity attributes. There is no disclosure of determining a positive or negative similarity match between at least one new user identity attribute and the denied user identity attributes based on similarity search results, allowing access for a negative match and denying access for a positive match, as claimed by Applicants, in the cited passages by the Office.

3. Regarding Applicants' claim 16, the Office believes that the Brown reference at column 14, lines 8-22 discloses the sixth element of Applicants' claim 16 of verifying a positive similarity match via a secondary review where a positive similarity match has been determined. The cited passage in the Brown reference describes use of record weights in a statistical analysis to determine whether there is a weighted match record that is sufficiently distinct in its weight to be considered a match for the input search data. There is no disclosure of the sixth element of Applicants' claim 16 in Chapman in combination with the passage in the Brown reference cited by the Office.

4. Regarding Applicants' claim 27, the Office asserts that Chapman discloses the eighth and ninth element of Applicants' claim 27 in the Chapman reference at column 4, lines 13-22, column 6 lines 23-35 and column 6, lines 56-64. Applicants can find no disclosure of a means for adding the new-user identity to the at least one database for storing valid user identities where a negative similarity match has been determined, and a means for adding the at least one new-user identity attribute to the at least one database of denied-user attributes where a positive similarity match has been determined in the passages cited by the Office.

5. Regarding Applicants claims 5-11, 13 and 20-24, the Office alleges that Chapman in combination with Brown at column 13, lines 27-30, column 14, lines 14-21, column 13, lines 27-30 and column 14, lines 14-17 discloses the elements of Applicants cited claims concerning a

first and second tolerance level. There in no disclosure in Chapman or Brown of a positive similarity match between the at least one new-user identity attribute and at least one denied-user identity attribute that meets or exceeds the first match tolerance level, and a negative similarity match between the at least one new-user identity attribute and at least one denied-user identity attribute that does not meet or exceed the first match tolerance level. There is also no disclosure in Chapman or Brown of allowing the new-user to access the computer system where the positive similarity match does not meet or exceed the second match tolerance level, and denying the new-user access to the computer system where the positive similarity match meets or exceeds the second match tolerance level.

Summary

The responses detailed above rebut the assertions by the Office of anticipation and obviousness of Applicants' invention, since all the elements of Applicants' claimed invention are not found in the cited references of Chapman et al, Brown et al and Berke. The responses substantiate the novelty and nonobviousness of claims 1-14, 16-25 and 27-31 over the cited references. Since the rejections are unsupported for failure to find all Applicants' claim limitations in the cited references, the rejections should be withdrawn. Allowance of the claims is requested.

Respectfully Submitted,

August 22, 2005
Date

Douglas D. Russell
Taylor Russell & Russell, P.C.
4807 Spicewood Springs Road
Building 2 Suite 250
Austin, Texas 78759
Tel. 512-338-4601